

Муниципальное бюджетное учреждение культуры «Ершичская централизованная библиотечная система» муниципального образования - Ершичский район

Смоленской области

Согласовано:

Председатель Ершичской

РПРК  Фомченкова Н.А.

Протокол № 1 от 10.01.2012 г.

Утверждаю:

Директор  Барасова Т.И.

«10» 01.2012 г.

## ПОЛОЖЕНИЕ

о защите персональных данных работников

### 1. Общие положения

1.1. Положение о защите персональных данных (далее - Положение) разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, главой 14 Трудового кодекса Российской Федерации, Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", иными нормативными актами, действующими на территории Российской Федерации.

1.2. Целью Положения является обеспечение защиты персональных данных работников от несанкционированного доступа, неправомерного их использования или утраты.

1.3. Положение о защите персональных данных (далее - Положение) определяет порядок сбора, хранения, комбинирования, передачи и любого другого использования персональных данных в соответствии с законодательством Российской Федерации.

1.4. Положение утверждается и вводится в действие приказом директора и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников.

1.5. Персональные данные относятся к категории конфиденциальной информации. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. Режим конфиденциальности персональных данных снимается в случаях прекращения деятельности организации, обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

### 2. Понятие и состав персональных данных

2.1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Персональные данные работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

2.2. В состав персональных данных работника входят:

- сведения, содержащиеся в документах, удостоверяющих личность;
- информация, содержащаяся в трудовой книжке;
- информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;
- сведения, содержащиеся в документах воинского учета;
- сведения об образовании, квалификации или наличии специальных знаний или подготовки;
- информация о состоянии здоровья в случаях, предусмотренных законодательством;
- сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации;
- сведения о семейном положении;
- информация о заработной плате;
- другая персональная информация.

### 3. Обработка персональных данных

3.1. Обработка персональных данных - любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

3.2. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

3.2.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.2.2. При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

3.2.3. Все персональные данные работника следует получать у него самого. Работодатель вправе обрабатывать персональные данные работников только с их письменного согласия. Форма письменного согласия утверждается директором ЦБС. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

3.2.4. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

3.2.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.3. Документы, содержащие персональные данные работника, создаются путём: копирования оригиналов (документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.); внесения сведений в учётные формы (на бумажных и электронных носителях); получения оригиналов необходимых документов (трудовая книжка).

3.4. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда договор заключается впервые, или работник поступает на работу на условиях совместительства, или трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для лиц, подлежащих воинскому учету;
- документ об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;
- свидетельство о присвоении ИНН (при его наличии у работника).

3.5. Работник обязан предоставлять работодателю достоверную персональную информацию. При изменении персональных данных работник должен письменно уведомить об этом работодателя в срок, не превышающий 14 дней. Работодатель имеет право запрашивать у работника дополнительные сведения и документы, подтверждающие их достоверность.

3.6. Порядок хранения и использования персональных данных работников устанавливается работодателем с соблюдением требований статей 86-89 Трудового кодекса Российской Федерации и иных федеральных законов.

3.7. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

3.8. Носители персональных данных.

3.8.1. Бумажные носители персональных данных:

- трудовая книжка,
- журналы учета трудовых книжек,
- журнал учета командировок,
- листки нетрудоспособности,
- материалы по учету рабочего времени,
- личная карточка Т-2,
- входящая и исходящая корреспонденция военкомата, страховой компании, службы судебных приставов,
- приказы по личному составу.

3.8.2. Электронные носители персональных данных - база данных по учету работников учреждения.

3.9. Персональные базы по учету на бумажных носителях хранятся в запираемом металлическом шкафу.

3.10. При наборе работников документы, находящиеся в работе сектора по работе с кадрами, могут находиться на рабочих столах или в специальных папках в течение рабочего дня. По окончании рабочего дня данные документы должны убираться в запирающие шкафы.

3.11. Персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК главного бухгалтера Отдела по культуре.

3.12. Персональные данные на электронных носителях защищены паролем доступа, доступ к специализированной программе осуществляется только через личный доступ пароль, право на использование персональных данных имеют только работники, ответственные за обработку персональных данных.

3.13. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.14. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

3.15. Передача персональных данных работника возможна только с согласия работника или в случаях, прямо предусмотренных законодательством.

3.16. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

3.16.1. не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;

3.16.2. не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

3.16.3. предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

3.16.4. разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

3.16.5. не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

3.16.6. передавать персональные данные работника представителям работника в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

3.17. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

3.18. При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы организации работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом.

3.19. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.20. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

3.21. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Работодатель учитывает личные качества работника, его добросовестный и эффективный труд.

#### 4. Доступ к персональным данным

4.1. Допуск к персональным данным работника разрешен должностным лицам, которым персональные данные необходимы для выполнения конкретных трудовых функций.

4.2. Внутренний доступ (доступ внутри учреждения);

4.2.1. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом директора учреждения.

4.3. Внешний доступ.

4.3.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

4.3.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

4.3.3. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

4.3.4. Другие организации.

Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением надлежащим образом заверенной копии заявления работника

4.3.5. Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

#### 5. Защита персональных данных

5.1. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем в порядке, установленном федеральным законом.

5.2. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5.3. Защита персональных данных представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности.

5.4. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

5.5. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

5.6. Внутренняя защита:

5.6.1. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами учреждения.

5.6.2. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с работниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел работников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только директору, работникам отдела управлением персоналом и в исключительных случаях, по письменному разрешению директора, - руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

5.7. Защита персональных данных работника на электронных носителях. Все папки, содержащие персональные данные работника, должны быть защищены паролем, который сообщается руководителю службы управления персоналом, заместителю директора по автоматизации, главному бухгалтеру.

5.8. Внешняя защита:

5.8.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, установка вредоносных программ (вирусов), подмена, фальсификация содержания реквизитов документа и др.

5.8.2. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе управления персоналом. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности учреждения, посетители, работники других организационных структур.

5.8.3. Для обеспечения внешней защиты персональных данных работника необходимо соблюдать ряд мер: технические средства охраны, сигнализации; требования к защите информации при интервьюировании и собеседованиях.

5.9. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

5.10. По возможности персональные данные обезличиваются.

5.11. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

## 6. Права и обязанности работника

6.1. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:

- на полную информацию о своих персональных данных и об обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом
- требовать исключения или исправления неверных или неполных персональных данных;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных;
- на обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

6.2. Работники и их представители должны быть ознакомлены под роспись с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

6.3. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

6.4. Работник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом Российской Федерации;
- своевременно сообщать работодателю об изменении своих персональных данных.

Работники ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

## 7. Уничтожение персональных данных

7.1. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

7.2. Персональные данные работников подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении таких целей.

## 8. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

8.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

8.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

8.3. Руководитель, разрешающий доступ работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

8.4. Каждый работник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

8.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

8.6. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

8.7. Должностные лица, в обязанность которых входит ведение персональных данных работника, обязаны обеспечить каждому работнику возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

8.8. В соответствии с Гражданским кодексом Российской Федерации лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.



3.

8.9. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказываются штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с Уголовным кодексом Российской Федерации.

8.10. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.